This exam has 6 questions on 10 pages, for a total of 50 points.

Duration: 60 minutes

- You need to show enough work to justify your answers.
- This is a closed-book examination. None of the following are allowed: documents or electronic devices of any kind (including calculators, cell phones, etc.)
- If your answers are not easily readable and well organized, they may not be read and credited.

LAST name: ____________________________________________

First name: : ____________________________________________

Student Number: _________________________________________

Signature: ______________________________________________

Instructor: Rachel Ollivier

<table>
<thead>
<tr>
<th>Question</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points:</td>
<td>20</td>
<td>15</td>
<td>10</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>50</td>
</tr>
<tr>
<td>Score:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Given a ring $R$, $R$-modules $A, B, C$ and morphisms of $R$-modules $A \xrightarrow{\alpha} B$ and $B \xrightarrow{\beta} C$ we recall that we have an exact sequence:

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

if

- $\alpha$ is injective,
- $\beta$ is surjective,
- $\text{im}(\alpha) = \ker(\beta)$.

It splits if there is a map $s : C \to A$ such that $\beta \circ s = \text{id}_C$.

We recall that a primitive polynomial in $\mathbb{Z}[X]$ is a non constant polynomial such that the gcd of its coefficients is 1.

The content of a non constant polynomial $P \in \mathbb{Q}[X]$ is the unique element $c(P) \in \mathbb{Q} \cap ]0, +\infty[\text{ such that } P = c(P)P_0$ where $P_0 \in \mathbb{Z}[X]$ is primitive. If $P$ is nonzero and constant, we set $c(P) = |P|$. We recall that $c$ is a multiplicative map $\mathbb{Q}[X] \setminus \{0\} \to \mathbb{Q} \cap ]0, +\infty[.$
1. Let $p$ be a prime number, $k$ a field, and let $R = k[X]/((X^2)(X - p))$. Recall that $k$ may have characteristic $p$.

   1. What are the morphisms of rings $R \to k$ which fix $k$?
   2. Give two sub-$R$-modules of $R$ which are not isomorphic to each other.

(b) Give morphisms of $k[X]$-modules which yield the following exact sequence

   \[ 0 \to k[X]/(X^2) \to k[X]/(X^2(X - p)) \to k[X]/(X - p) \to 0. \]

Does it split? Justify your answer.

1. (a) By precomposition by $k[X] \to R \quad \overset{d}{\longrightarrow} \quad R \mod X^2(X-p)$

   a morphism of rings $k [X] \to k$ fixing $k$

   Such morphisms are determined by the image of $X$ and they are of the form

   \[ k[X] \longrightarrow k \]

   \[ P \longrightarrow P(d) \]

   So the morphisms $R \to k$ fixing $k$ arise from morphisms $k[X] \to k$ the kernel of which contains $X^2(X-p)$

   namely $d^2(d-p) = 0$

   So $d = 0 \quad \text{or} \quad d = p$.

   Answer: $R \longrightarrow k \quad \overset{P\mod X^2(X-p)}{\longrightarrow} P(0) \quad \overset{P\mod X^2(X-p)}{\longrightarrow} P(d)$

2. Example: \[ \frac{(X)}{(X^2)(X-p)} \quad \text{and} \quad \frac{(X^2)}{(X^2)(X-p)} \]

   are two ideals of $R$, so they are sub-$R$-modules

   the first one is a 2 dimensional $k$-vector space,

   the second one a 1 dimensional $k$-vector space

   so they are not isomorphic as $R$-modules (because otherwise they would be isomorphic as $k$-modules).
b) \( \mathbb{A}^2 \longrightarrow \mathbb{A}^2 / X^2(\lambda-x) \) is a morphism
\[ \mathbb{P} \longrightarrow (\lambda-x) \mathbb{P} \mod X^2(\lambda-x) \]

The kernel is \( X^2 \mathbb{A}^2 \) so it yields an injective map:
\[ \mathbb{A}^2 / X^2(\lambda-x) \longrightarrow \mathbb{A}^2 / X^2(\lambda-x) \]
\[ \mathbb{P} \mod X^2(\lambda-x) \longrightarrow \mathbb{P} \mod X^2(\lambda-x) \]

The reduction map \( \mathbb{A}^2 \longrightarrow \mathbb{A}^2 / X^2 \) is surjective. Its kernel contains \( X^2(\lambda-x) \) so it yields a surjective map:
\[ \mathbb{A}^2 / X^2(\lambda-x) \longrightarrow \mathbb{A}^2 / X^2(\lambda-x) \]
\[ \mathbb{P} \mod X^2(\lambda-x) \longrightarrow \mathbb{P} \mod X^2(\lambda-x) \]

If \( \text{char } \mathbb{k} \neq \lambda \), let \( \mathbb{A}^2 \longrightarrow \mathbb{A}^2 / X^2 \)
\[ \mathbb{P} \longrightarrow 1 X^2 X^2 \mod X^2(\lambda-x) \]

It is a morphism of \( \mathbb{A}^2 \)-modules whose kernel contains \( (\lambda-x) \) so it yields a morphism:
\[ \mathbb{A}^2 / (\lambda-x) \longrightarrow \mathbb{A}^2 / X^2 \]
\[ \mathbb{P} \mod X-x \longrightarrow 1 X^2 X^2 Y^2 \mod X^2(\lambda-x) \]

Notice: \( \mathbb{P} \mod (\lambda-x) = 1 X^2 X^2 \mod X^2 = \mathbb{P} \mod X^2 \)

So for \( x = \lambda \) and \( \mathbb{P} \mod X-x \) the sequence splits.

If \( \text{char } \mathbb{k} = \lambda \), the sequence does not split otherwise.

\[ \mathbb{A}^2 / X^3 = \mathbb{A}^2 / Y^2 \oplus \mathbb{A}^2 / X \]

as a \( \mathbb{A}^2 \)-module so \( \mathbb{A}^2 / X^3 \) would be annihilated by \( X^2 \)
2. (a) Show that $\sqrt{2}$ (resp. $\sqrt{3}$) is an algebraic integer namely there is a monic polynomial in $\mathbb{Z}[X]$ which has $\sqrt{2}$ (resp. $\sqrt{3}$) as a root.

(b) Show that $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ is a quotient of a free $\mathbb{Z}$-module of rank 4 namely there is a surjective morphism of abelian groups

$$\mathbb{Z}^4 \to \mathbb{Z}[\sqrt{2}, \sqrt{3}].$$

Give explicitly the image $u_1, u_2, u_3, u_4$ of the canonical basis $e_1, e_2, e_3, e_4$ of $\mathbb{Z}^4$ in $\mathbb{Z}[\sqrt{2}, \sqrt{3}].$

(c) Let $\alpha := \sqrt{2} + \sqrt{3}$. Compute $\alpha u_4$ in terms of $\{u_i\}_{1 \leq i \leq 4}$.

(d) Find a monic polynomial in $\mathbb{Z}[X]$ which has $\alpha$ as a root.

(e) What is the ideal $\{P \in \mathbb{Q}[X], P(\alpha) = 0\}$? Justify your answer.

\[(a) \quad X^2 - 2, \quad X^3 - 3 \]

\[(b) \quad \mathbb{Z}^4 \to \mathbb{Z}[\sqrt{2}, \sqrt{3}], \quad (x_1, x_2, x_3, x_4) \mapsto x_1 u_1 + 2x_2 u_2 + 3x_3 u_3 + 2x_4 u_4 \]

where $u_1 = 1, \quad u_2 = \sqrt{2}, \quad u_3 = \sqrt{3}, \quad u_4 = \sqrt{6}$.

We have a surjective morphism of abelian groups since for $a, b \geq 1$

we have $a = 2a' + r$, $b = 2b' + s$ (Euclidean division) such that $r, s \in \{0, 1\}$

and $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$ is in the image of the morphism above.

\[(c) \quad \begin{align*}
\delta u_1 &= u_2 + u_3 \\
\delta u_2 &= 2u_1 + u_4 \\
\delta u_3 &= 3u_1 + u_4 \\
\delta u_4 &= 2u_2 + 2u_3
\end{align*} \]

\[(d) \quad M = \begin{pmatrix}
\alpha_1 & 0 \\
0 & \alpha_2 \\
0 & 0 \\
0 & 1
\end{pmatrix}
\]

So $\delta$ is a root for $\det(\chi I - M) \in \mathbb{Z}[X]$

which is okay too (and actually gives the same result):

$(a - \sqrt{2})^2 = (\sqrt{3})^2$ so $a^2 - 2\sqrt{2}a + 1 = 0$

$2\sqrt{2}a = 1 - a^2$ and $8a^2 = (1 - a^2)^2$ which gives $a^4 - 10a^2 + 1 = 0$. 

\[(e) \quad \text{monic}\]
(e) We have to describe the Kernel of
\[ \mathbb{Q}[x] \rightarrow \mathbb{Q}[a] \]
\[ P \rightarrow P(a) \]
It is generated by a polynomial \( A \in \mathbb{Q}[x] \setminus \{0\} \) and contains \( P_0 = \det \begin{pmatrix} xI - M \end{pmatrix} \), so \( A \) divides \( P_0 \) — deg \( A \leq 4 \)

But \( \deg A = \dim \mathbb{Q}[a] \)

\[ \mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[x] \]

FIELD and \( \mathbb{Q} \)-vector spaces:
\[ \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[x] \rightarrow \mathbb{Q}[\sqrt{2}] \]

Remark: using the Euclidean algorithm to find a Bezout identity between the polynomial 2\( x \) and the polynomial \( P_0 \) (why are they coprime?) you can even give the explicit expression of \( 1/2a \) as a polynomial expression in \( a \) (please try!) (See Midterm 1 Question 3 (e) which I encourage you to look into carefully.)

Likewise try to write \( 1/(1+a+a^2) \) for example as a polynomial expression in \( a \).

So \( \deg A = 4 \) and \( (A) = (P_0) \)
3. Let $g \in \mathbb{Z}[X]$ be a non-constant polynomial. We are going to show that $\mathbb{Z}[X]/g\mathbb{Z}[X]$ is not a field.

(a) What is the characteristic of the ring $\mathbb{Z}[X]/g\mathbb{Z}[X]$?

(b) Show that there is $a \in \mathbb{Z}$ such that $g(a) \neq 0, \pm 1$ and let $p$ be a prime number dividing $g(a)$.

(c) Show that there is a unique well defined surjective morphism of rings $\mathbb{Z}[X] \rightarrow \mathbb{Z}/p\mathbb{Z}$ sending $X$ onto $a \mod p$ and that it factors through $\mathbb{Z}[X]/g\mathbb{Z}[X]$.

(d) Show that the resulting map $\varphi : \mathbb{Z}[X]/g\mathbb{Z}[X] \rightarrow \mathbb{Z}/p\mathbb{Z}$ is not injective.

(e) Conclude.

\[ a) \quad \mathbb{Z} \xrightarrow{\text{is injective}} \mathbb{Z}[X]/g\mathbb{Z}[X] \xrightarrow{\text{mod } g\mathbb{Z}[X]} \]

Since $g$ is not constant so $\text{char } \mathbb{Z}[X]/g\mathbb{Z}[X] = 0$.

\[ b) \quad g \text{ is not constant so } \lim_{x \to \pm 0} g(x) = \pm a \]

and for $a \in \mathbb{Z}$ large enough we have $|g(a)| > 2$.

So if $p$ prime $p$ divides $g(a)$.

\[ c) \quad \mathbb{Z}[X] \rightarrow \mathbb{Z}/p\mathbb{Z} \quad \text{send } X \rightarrow P(a) \mod p \]

its kernel contains $g$ so there is a morphism of rings $\mathbb{Z}[X] \rightarrow \mathbb{Z}/p\mathbb{Z}$, $P \rightarrow P(a) \mod p$.\[ \rightarrow P(a) \mod p \]}
1) If \( \mathbb{Z}[x]/g \mathbb{Z}[x] \to \mathbb{Z}/p \mathbb{Z} \) was injective, the ring \( \mathbb{Z}[x]/g \mathbb{Z}[x] \) would have characteristic \( p \). (Note that it is not reduced to \( 103 \) since \( g \) is not constant.)

2) If \( \mathbb{Z}[x]/g \mathbb{Z}[x] \) was a field, the map \( \mathbb{Z}[x]/g \mathbb{Z}[x] \to \mathbb{Z}/p \mathbb{Z} \) which is not the zero map would be injective since a field has only itself or \( 0 \) as ideals.
4. Let \( f \in \mathbb{Z}[X] \) primitive. Show that \((f \mathbb{Q}[X]) \cap \mathbb{Z}[X] = f\mathbb{Z}[X]\).

\[ \text{is clear.} \]

\( \text{Let } \mathbb{P} \in \mathbb{Q}[X] \)

\[ \text{and suppose } f\mathbb{P} \subset \mathbb{Z}[X]. \]

\[ \implies c(f\mathbb{P}) = c(f)c(\mathbb{P}) = c(\mathbb{P}) \subset \mathbb{Z} \]

So, \( c(\mathbb{P}) \subset \mathbb{Z} \)

But \( \mathbb{P} = c(\mathbb{P}) \mathbb{P}_0 \)

Where \( \mathbb{P}_0 \subset \mathbb{Z}[X] \) (primitive)

So, \( \mathbb{P} \in \mathbb{Z}[X] \)

And \( f\mathbb{P} \subset f\mathbb{Z}[X] \).